ОБ ИЗОМЕТРИЧНОСТИ ПЛОТНО УПАКОВАННЫХ БИНАРНЫХ КОДОВ*)

С. В. Августинович

В работе изучается изометричность плотно упакованных (соверше
ных) бинарных кодов длины n с кодовым расстоянием 3. Как установи
Г. С. Шапиро и Д. Л. Злотник [1], в любом плотно упакованном $(n,3)$-ко
число кодовых вершин, находящихся на фиксированном расстоянии
данной кодовой вершины, не зависит от выбора этой вершины и от выбо
кода. В связи с этим в [1] высказано предположение о единственности
точностью до эквивалентности плотно упакованных $(n,3)$-кодов для тех
при которых такие коды существуют, т. е. для $n = 2^k - 1$ $(k = 1, 2, 3, ..$
Это предположение опроверг Ю. Л. Васильев (см. [2]), построив больш
число неэквивалентных $(n,3)$-кодов для любого $n = 2^k - 1$ $(k \geqslant 4)$. Т
не менее до последнего времени предполагалось (см., например, [3]), ч
при каждом $n = 2^k - 1$ все плотно упакованные $(n,3)$-коды изометрич
(хотя имеются неэквивалентные). В настоящей заметке доказывается, ч
любые два изометричных плотно упакованных $(n,3)$-кода эквивалентн

Пусть E^n — единичный n-мерный куб, образованный булевыми пер
менными $x_1, \ldots, x_n$, $\mathcal{Z}$ — множество вершин куба E^n. Каждой верши
$\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathcal{Z}$ сопоставим множество $\hat{\alpha}$ переменных, которые в
принимают значение единица. Например, если $\tilde{\alpha} = (1, 1, 0, 1, 0, \ldots, 0)$,
$\hat{\alpha} = \{x_1, x_2, x_4\}$. Ясно, что все $\hat{\alpha} \subset X$, где $X = \{x_1, \ldots, x_n\}$ — множест
переменных.

- Подмножества Z_1 и Z_2 множества $\mathcal{Z}$ одинаковой мощности *эквив*
лентны, если существует перестановка σ переменных $x_1, \ldots, x_n$
кая, что порождаемое этой перестановкой отображение $J_\sigma: E^n \to$
переводит Z_1 в Z_2.
- Отображение $I\colon Z_1 \to Z_2$ (вообще говоря, не зависящее от автомо
физмов куба E^n) называется *изометрией*, если для любых $\tilde{\alpha}$, $\tilde{\beta} \in$
выполняется равенство $d(\tilde{\alpha}, \tilde{\beta}) = d(I(\tilde{\alpha}), I(\tilde{\beta}))$, где d — расстоян
Хэмминга.

В силу равномощности множеств Z_1 и Z_2 все свойства изометрии, о
видно, обратимы. Для простоты в дальнейшем предполагаем, что $\tilde{0} \in$
$\tilde{0} \in Z_2$ и $I(\tilde{0}) = \tilde{0}$. Легко построить примеры неэквивалентных изометри
ных подмножеств куба E^n (см. [3]).

---

*) Работа выполнена при финансовой поддержке Российского фонда фундамента
ных исследований (код проекта 973-011-1484).

- Подмножество $Z = \{\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k\}$ множества вершин $\mathcal{Z}$ называется *плотно упакованным* $(n,3)$*-кодом*, если
  - $d(\tilde{\alpha}_i, \tilde{\alpha}_j) \geqslant 3$ при $i \neq j$,
  - для $\tilde{\alpha} \in E^n$ и $\tilde{\alpha} \notin Z$ существует единственное число i такое, что $d(\tilde{\alpha}, \tilde{\alpha}_i) = 1$.

Непосредственно из определения плотно упакованного кода вытекают следующие предложения.

Предложение 1. *Пусть Z — плотно упакованный $(n,3)$-код и $\tilde{\alpha}$ — кодовая вершина ($\tilde{\alpha} \in Z$). Тогда для любых i, j ($i \neq j$) существует единственное число k такое, что при замене значений i-, j-, k-й координат $\tilde{\alpha}$ на противоположные ($0 \leftrightarrow 1$) снова получается кодовая вершина $\tilde{\alpha}^*$.*

- В условиях предложения 1 будем говорить, что *в направлении (i,j,k) от вершины $\tilde{\alpha}$ лежит кодовая вершина $\tilde{\alpha}^*$.*

Предложение 2. *Пусть $\tilde{\alpha} \in Z$ и $1 \leqslant i \leqslant n$. Тогда множество $X \setminus \{x_i\}$ единственным образом разбивается на пары $(x_{i_1}, x_{i_2}), \ldots, (x_{i_{n-2}}, x_{i_{n-1}})$ такие, что в направлении (i, i_{2t-1}, i_{2t}) от вершины $\tilde{\alpha}$ лежит некоторая другая кодовая вершина.*

Из предложения 2, в частности, следует, что для четных n не существует плотно упакованных $(n,3)$-кодов.

Лемма. *Пусть $\widehat{\alpha}_1, \ldots, \widehat{\alpha}_l$ ($l > 7$) — семейство трехэлементных множеств и $|\widehat{\alpha}_i \cap \widehat{\alpha}_j| = 1$ при $i \neq j$. Тогда существует единственный элемент x, принадлежащий сразу всем множествам семейства.*

Доказательство. Рассмотрим множество $\widehat{\alpha}_i$ и его элемент x, который принадлежит наибольшему числу из оставшихся множеств семейства. Ввиду ограничения $l > 7$ имеется не менее трех таких множеств. Поэтому по крайней мере четыре множества пересекаются по элементу x. Всякое множество, не содержащее x, должно пересекаться с этими четырьмя по другим элементам и потому должно содержать не менее четырех различных элементов; противоречие. Следовательно, все множества семейства содержат x. □

Заметим, что при $l \leqslant 7$ лемма неверна, как показывает пример:

$$\{123\}, \{145\}, \{167\}, \{246\}, \{257\}, \{347\}, \{356\}.$$

Теорема. *Пусть $n > 15$. Если два плотно упакованных $(n,3)$-кода $Z_1 = \{\tilde{\alpha}_0, \ldots, \tilde{\alpha}_r\}$ и $Z_2 = \{\tilde{\alpha}'_0, \ldots, \tilde{\alpha}'_r\}$ изометричны, то они эквивалентны.*

Доказательство. Пусть I — изометрия, переводящая Z_1 в Z_2. Не теряя общности, можно считать, что $I(\alpha'_i) = \alpha'_i$ для всех i ($i \leqslant r$), причем $\tilde{\alpha}_0 = \tilde{\alpha}'_0 = \tilde{0}$. Рассмотрим произвольную переменную $x \in X$ и выделим в коде Z_1 нулевую вершину. Согласно предложению 2 в Z_1 существует $m = n(n-1)/2 > 7$ кодовых вершин $\tilde{\alpha}_{i_1}, \ldots, \tilde{\alpha}_{i_m}$, имеющих ровно три ненулевых координаты, одна из которых есть x, а остальные образуют разбиение множества $X \setminus \{x\}$ на непересекающиеся пары $P_1, \ldots, P_m$. По определению изометрии образы $\tilde{\alpha}'_{i_1}, \ldots, \tilde{\alpha}'_{i_m}$ вершин $\tilde{\alpha}_{i_1}, \ldots, \tilde{\alpha}_{i_m}$ находятся на расстоянии 3 от вершины $\tilde{0}$ и на расстоянии 4 друг от друга. Рассматривая эти вершины как трехэлементные множества переменных, можно применить лемму, согласно которой найдется переменная x' такая,

что множества $\widehat{\alpha}'_{i_1}, \ldots, \widehat{\alpha}'_{i_m}$ пересекаются по x'. Ясно, что каждой переменной $x \in X$ можно поставить в соответствие переменную x', причем это соответствие будет перестановкой на множестве X. Обозначим эту перестановку через σ. Таким образом, σ задает автоморфизм куба E^n.

Покажем, что для всех кодовых вершин из Z_1 действие указанного автоморфизма совпадает с I. Зафиксируем произвольное $\widehat{\alpha} \in Z_1$. Рассуждая от противного, предположим, что для некоторого i выполняется включение $x_i \in \widehat{\alpha}$, но $\sigma(x_i) \notin I(\widehat{\alpha})$. Рассмотрим те вершины $\widetilde{\alpha}_{i_1}, \ldots, \widetilde{\alpha}_{i_m}$ кода Z_1, вес которых равен 3 и $x_i = 1$. Как было отмечено выше, двухэлементные множества $P_1 = \{\widehat{\alpha}_{i_1} \setminus \{x_i\}\}, \ldots, P_m = \{\widehat{\alpha}_{i_m} \setminus \{x_i\}\}$ не пересекаются и вместе с одноэлементным множеством $\{x_i\}$ покрывают X. Поэтому

$$|\widehat{\alpha}| = 1 + \sum_{j=1}^{m} |\widehat{\alpha} \cap P_j| = 1 + \sum_{j=1}^{m} |\widehat{\alpha} \cap \widehat{\alpha}_{i_j}| - m.$$

С другой стороны, в силу условия $\sigma(x_i) \notin I(\widehat{\alpha}) = \widehat{\alpha}'$ имеем

$$|\widehat{\alpha}| = |\widehat{\alpha}'| = \sum_{j=1}^{m} |\widehat{\alpha}' \cap \widehat{\alpha}'_{i_j}| = \sum_{j=1}^{m} |\widehat{\alpha} \cap \widehat{\alpha}_{i_j}|,$$

что противоречит предыдущему равенству.

Замечание 1. Теорема останется верной, если в ее формулировке условие изометричности кодов заменить на условие слабой изометричности, т. е. потребовать, чтобы отображение I сохраняло лишь минимальные расстояния Хэмминга для плотно упакованных кодов без каких-либо условий на вершины, находящиеся на расстоянии больше трех.

Замечание 2. В доказательстве теоремы существенно использовалось существование троек Штейнера среди вершин третьего уровня множества Z_1. Теорема верна и для всех других изометричных множеств, обладающих таким свойством.

Замечание 3. В случае $n = 15$, по мнению автора, изометричных неэквивалентных кодов не существует.

ЛИТЕРАТУРА

1. **Шапиро Г. С., Злотник Д. Л.** К математической теории кодов с исправлением ошибок // Кибернетический сб. 1962. № 5. С. 7–32.
2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Наука, 1962. Вып. 8. С. 337–339.
3. **Абдурахманов Ж. К.** О геометрической структуре кодов, исправляющих ошибки: Дис. ... канд. физ.-мат. наук: 01.01.09. Ташкент, 1991. С. 66.